Security chip for data protection

Patent Number:	DE19539700
Publication date:	1996-11-28
Inventor(s):	EBERHARD GUENTHER DIPL PHYS (DE); GESNER JUERGEN DIPL PHYS (DE); MOELLER WOLF-DIETRICH DR ING (DE); SCHAEFER MANFRED DR ING (DE)
Applicant(s):	SIEMENS AG (DE)
Requested Patent:	☑ DE19539700
Application Number:	DE19951039700 19951025
Priority Number (s):	DE19951039700 19951025
IPC Classification:	G06F19/00; G06K19/07; H04L9/00
EC Classification:	G07F7/10D4E, H04L9/00
Equivalents:	☐ EP0857382 (WO9716003), JP11513864T, ☐ RU2180987, ☐ WO9716003

Abstract

The invention relates to a security chip (SC) which is disconnected from application hardware (AHW) and only connected to the application hardware (AHW) by way of a data interface (DS) and a command interface (BS). The security chip (SC) has its own processor (P) and a plurality (VZ) of independent algorithm modules (AMi) for carrying out symmetric encryption algorithms (SV) and/ or asymmetric encryption algorithms (AV), all components of the security chip (SC) being connected via a bus (IB) inside the chip. The methods for encryption management and for cryptographic user data processing are carried out together on the security chip (SC), and consequently the security features of said chip (SC) are considerably improved in relation to known arrangements.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(10) **DE 195 39 700 C 1**

(51) Int. Cl.[6]:
G 06 F 19/00
G 06 K 19/07
H 04 L 9/00

(21) Aktenzeichen: 195 39 700.2-53
(22) Anmeldetag: 25. 10. 95
(43) Offenlegungstag: —
(45) Veröffentlichungstag der Patenterteilung: 28. 11. 96

DE 195 39 700 C 1

(73) Patentinhaber:
Siemens AG, 80333 München, DE

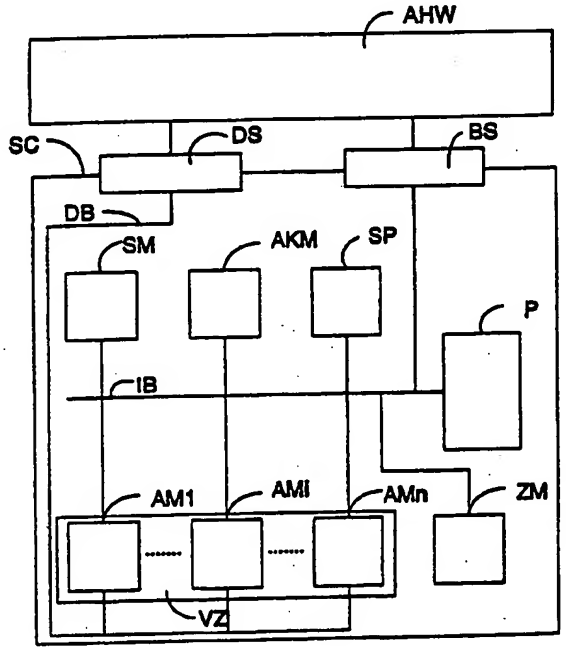
(72) Erfinder:
Eberhard, Günther, Dipl.-Phys., 82223 Eichenau, DE;
Geßner, Jürgen, Dipl.-Phys., 85521 Ottobrunn, DE;
Moeller, Wolf-Dietrich, Dr.-Ing., 81739 München, DE;
Schäfer, Manfred, Dr.-Ing., 85661 Forstinning, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

GOLDBERG, L.: New Encryption strategy uses hardware and software to protect data on public networks, Electronic Design, März 1995, S. 39-40;
EBERHARD, G.: Zwei neue Kryptoprodukte von Siemens:..., IS-Aktuell, April 1993, S. 7-17 bis 7-18;

(54) **Sicherheitschip**

(57) Ein Sicherheitschip (SC) ist von einer Anwendungshardware (AHW) entkoppelt und nur über eine Datenschnittstelle (DS) und über eine Befehlsschnittstelle (BS) mit der Anwendungshardware (AHW) verbunden. Der Sicherheitschip (SC) weist einen eigenen Prozessor (P) und eine Vielzahl (VZ) unabhängiger Algorithmenmodule (AMI) zur Durchführung von symmetrischen Verschlüsselungsalgorithmen (SV) und/oder asymmetrischen Verschlüsselungsalgorithmen (AV) auf, wobei alle Komponenten des Sicherheitschips (SC) über einen chipinternen Bus (IB) gekoppelt sind.
Durch die Tatsache, daß die Verfahren zur Schlüsselverwaltung und zur kryptographischen Nutzdatenverarbeitung auf dem Sicherheitschip (SC) zusammen durchgeführt werden, werden die Sicherheitseigenschaften des Sicherheitschips (SC) gegenüber bekannten Anordnungen erheblich verbessert.



DE 195 39 700 C 1

Beschreibung

Zur Wahrung der Sicherheit von Kommunikationsbeziehungen, beispielsweise von Datenkommunikation oder auch Sprachkommunikation, werden kryptographische Algorithmen zur Verschlüsselung der eigentlichen Kommunikationsdaten eingesetzt. Verschiedene Algorithmen dienen beispielsweise zur Sicherung der Integrität, der Vertraulichkeit oder der Authentizität der übertragenen Daten oder auch der Kommunikationspartner.

Es werden also Sicherheitschips benötigt, die die kryptographischen Verfahren und Protokolle für verschiedenste informationstechnische Anwendungen durchführen.

Es sind spezielle, für einzelne Anwendungen ausgerichtete Sicherheitsmodule bekannt, beispielsweise ein Sicherheitsmodul für sichere Telefaxübertragungen (Siemens, Datensicherungsmodul DSM-Fax, sichere Faxübertragungen, Siemens Bereich Sicherungstechnik) oder auch zur Verschlüsselung von Telefongesprächen (Siemens, DSM-Voice-Telephoning in Confidence, Siemens Bereich Sicherungstechnik; Luis Cypher, LC-1 Der digitale Sprachverschlüssler für abhörsicheres Telefonieren).

Weiterhin sind spezielle, für asymmetrische Kryptoalgorithmen entwickelte Chipkartencontroller und Coprozessoren bekannt (IS-Aktuell, Produkte/Systeme, S. 7—17 bis 7—18, April 1993, 1993).

Es sind weitere Sicherheitschips bekannt, bei dem entweder der symmetrische Kryptoalgorithmus hardwareunterstützt durchgeführt wird, aber der asymmetrische Kryptoalgorithmus nur von der Software unterstützt wird, oder umgekehrt (L. Goldberg, New Encryption strategy uses hardware and software to protect data on public networks, Electronic Design, S. 39—40, März 1995; G. Eberhard, Zwei neue Kryptoprodukte von Siemens: der Chipkartenkontroller SLE44C200 und der Coprozessor SLE44CP2, Prozessoren für asymmetrische Algorithmen, IS-Aktuell, S. 7—17 — 7—18, April 1993).

Diese bekannten Sicherheitsmodule weisen den Nachteil auf, daß sie jeweils nur auf ganz bestimmte Anwendungen eingeschränkt sind. Vor allem ist jeweils entweder nur ein asymmetrischer Algorithmus, die beide direkt hardwareunterstützt ablaufen, für die Datenverschlüsselung auf einem einzigen Sicherheitschip vorgesehen oder nur eine symmetrische Datenverschlüsselung auf einem Chip.

Diese Einschränkung führt zu einem weiteren Nachteil der bisherigen Lösungen, daß sicherheitskritische Information in einer die Verschlüsselungsalgorithmen durchführenden Recheneinheit teilweise noch über einen ungesicherten Bus der Recheneinheit übertragen wird, beispielsweise bei der Schlüsselverwaltung kryptographischer Schlüssel und der Übertragung von Nutzdaten und somit von einem Angreifer abgefangen werden kann.

Somit liegt der Erfindung das Problem zugrunde, einen Sicherheitschip anzugeben, der die im vorigen genannten Nachteile vermeidet.

Das Problem wird durch den Sicherheitschip gemäß Patentanspruch 1 gelöst.

Der Sicherheitschip ist von der Anwendungshardware komplett abgekoppelt und nur über eine Datenschnittstelle und eine Befehlsschnittstelle "ansprechbar". Da der Sicherheitschip einen eigenen Prozessor, einen chipinternen Bus, auf den die Anwendungshardware

nicht zugreifen kann, sowie unterschiedliche Algorithmenmodule, mit denen die verschiedensten Sicherheitsdienste, basierend auf asymmetrischen und symmetrischen Algorithmen durchgeführt werden, aufweist, ist der Sicherheitschip universell anwendbar und gibt keinerlei sicherheitsrelevante Information an die Anwendungshardware.

Dadurch kann die Anwendungshardware und die Anwendungssoftware beliebig geladen, konfiguriert und angepaßt werden, ohne daß die Sicherheit der verschiedenen Kryptofunktionen, die mit den Algorithmenmodulen durchgeführt werden, gefährdet ist.

Durch die Weiterbildung des Sicherheitschips gemäß Patentanspruch 5 ist es möglich, Angriffe auf den Sicherheitschip zu erkennen und auch eventuell darauf beispielsweise mit einer Löschung aller Daten, zu reagieren.

Die Weiterbildung des Sicherheitschips gemäß Patentanspruch 6 realisiert eine Erweiterung der Algorithmenmodule um weitere Sicherheitsdienste und erweitert somit die Anwendbarkeit des Sicherheitschips.

Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Ein bevorzugtes Ausführungsbeispiel der Erfindung ist in den Zeichnungen dargestellt und wird im folgenden näher beschrieben.

Es zeigen

Fig. 1 eine Skizze, die eine mögliche Anordnung des Sicherheitschips beschreibt;

Fig. 2 ein Blockdiagramm, das mögliche Algorithenmodule beschreibt;

Fig. 3 eine Anordnung, die den Aufbau eines sicheren Zeitgebermoduls darstellt.

Anhand der **Fig. 1** bis 3 wird die Erfindung weiter erläutert.

In **Fig. 1** ist eine Anordnung eines Sicherheitschips SC dargestellt.

Der Sicherheitschip SC weist mindestens folgende Komponenten auf:

- einen Prozessor P,
- eine Vielzahl VZ von unabhängigen Algorithmenmodulen AMi zur Durchführung von Verschlüsselungsalgorithmen,
- einen Speicher SP,
- eine Datenschnittstelle DS, die von der Performance des Prozessors P unabhängig ist,
- eine sichere Befehlsschnittstelle BS, die entweder in einen chipinternen Datenbus DB oder direkt in den Prozessor P geführt ist,
- den chipinternen Datenbus DB, über den die Vielzahl VZ von unabhängigen Algorithmenmodulen AMi mit der Datenschnittstelle DS gekoppelt ist, und
- einen chipinternen Bus IB, mit dem alle Komponenten bis auf die Datenschnittstelle DS gekoppelt sind.

Durch die Abkopplung der Datenschnittstelle DS von dem chipinternen Bus IB istm die Verschlüsselungsleistung nicht mehr abhängig von dem Prozessor P. Außerdem können die chipinternen Daten von dem chipinternen Bus IB nicht von einem unbefugten Dritten insbesondere an der Datenschnittstelle DS nicht abgehört bzw. manipuliert werden.

Weiterhin kann der Sicherheitschip SC folgende Komponenten aufweisen:

- ein Zeitgebermodul ZM,
- ein Sensorikmodul SM und
- ein Aktorikmodul AKM.

Auch diese Komponenten sind mit dem chipinternen Bus IB gekoppelt.

Zur Kommunikation zwischen den einzelnen Komponenten, also zur Ablaufsteuerung, können unterschiedlichste Kommunikationsprotokolle, selbstverständlich unabhängig von dem von einer Anwendungshardware AHW verwendeten Kommunikationsprotokoll, eingesetzt werden.

Die Datenschnittstelle DS und die Befehlsschnittstelle BS sind die einzigen Zugriffspunkte für die Anwendungshardware AHW auf den Sicherheitschip SC.

Auf eine andere Weise hat die Anwendungshardware AHW keine Möglichkeit, auf den Sicherheitschip SC und somit auch auf die sicherheitsrelevanten Daten, die in dem Sicherheitschip SC verwendet und/oder gespeichert werden, zuzugreifen.

Durch diese Abkopplung des Sicherheitschips SC von seiner "Außenwelt" ist es für einen unbefugten Dritten, also einen Angreifer, nicht mehr möglich, sicherheitsrelevante Daten irgendeiner Art von dem Sicherheitschip SC zu erhalten.

Der Prozessor P kann ein beliebiger Prozessor mit einer geeigneten Geschwindigkeit sein, die sich direkt aus den Anforderungen der geplanten Anwendung ergibt.

Die Algorithmenmodule AMi sind unabhängige Module, von denen jedes jeweils speziell für ein kryptographisches Protokoll bzw. Verfahren "zuständig" ist. Darunter sind beispielsweise Verfahren oder Protokolle zur Verschlüsselung und Entschlüsselung von Nutzdaten, zum Integritätsschutz, oder auch zur digitalen Unterschrift (Signatur) oder Hashwertbildung zu verstehen. Der Index i identifiziert jedes Algorithmenmodul AMi eindeutig. Er ist eine beliebige natürliche Zahl im Bereich von 1 bis n. Hierbei ist n die Anzahl der verschiedenen, auf dem Sicherheitschip SC realisierten Algorithmenmodule AMi.

Mögliche Ausführungsbeispiele für die Algorithmenmodule AMi werden im folgenden erläutert.

Ein Algorithmenmodul AMi ist beispielsweise ein Modul, das speziell zur Durchführung eines kryptographischen symmetrischen Verfahrens SV, beispielsweise des Data Encription Standard-Verfahrens (DES-Verfahrens) vorgesehen ist. Das Modul kann auch so ausgelegt sein, daß es das DES-Verfahren mit unterschiedlichen Schlüssellängen, also zum Beispiel auch das Triple-DES-Verfahren durchführen kann. Weitere symmetrische kryptographische Verfahren SV erfahren können in weiteren Algorithmenmodulen AMi realisiert sein.

In einem weiteren Ausführungsbeispiel ist es vorgesehen, in den Algorithmenmodulen AMi auch asymmetrische kryptographische Algorithmen AV durchzuführen. Beispiele für asymmetrische kryptographische Algorithmen AV sind jedem Fachmann hinlänglich bekannt, beispielsweise das RSA-Verfahren.

Diese im vorigen beschriebenen symmetrischen Verschlüsselungsalgorithmen SV und asymmetrischen kryptographischen Algorithmen AV können sowohl gesondert als auch zusammen in unterschiedlichen Algorithmenmodulen AMi auf dem Sicherheitschip SC vorgesehen sein.

Es können auch mehrere Algorithmenmodule AMi gleicher Bauart zur Durchführung des jeweils gleichen Verfahrens auf dem Sicherheitschip SC vorgesehen sein, beispielsweise zur Erhöhung des Performance des Sicherheitschips SC. Dies kann z. B. auch in einer Art vorgesehen sein, daß ein Algorithmenmodul AMi zur Verarbeitung eines ankommenden Datenstroms und ein anderes Algorithmenmodul AMi gleicher Bauart zur Verarbeitung eines abgehenden Datenstroms vorgesehen ist.

Die Algorithmenmodule AMi dienen unter anderem der Verschlüsselung von Nutzdaten, die über die Datenschnittstelle DS in Klartext von der Anwendungshardware AHW auf einen chipinternen Datenbus DB gelegt werden und mit einem beliebigen, von der Anwendungshardware AHW über die Befehlsschnittstelle BS festgelegten Verschlüsselungsverfahren, durch das auch das verwendete Algorithmenmodul AMi aus der Vielzahl VZ der unabhängigen Algorithmenmodule AMi ausgewählt wird, verschlüsselt werden.

Die in dem jeweiligen Algorithmenmodul AMi verschlüsselten Nutzdaten werden wieder über den chipinternen Datenbus DB und die Datenschnittstelle DS, nun in verschlüsselter Form, zu der Anwendungshardware AHW übertragen.

Über die Befehlsschnittstelle BS wird durch die Anwendungshardware AHW dem Sicherheitschip SC die Parameter der jeweiligen Verschlüsselungsanforderung für die Nutzdaten bekanntgegeben. Dies können beispielsweise der zu verwendende Verschlüsselungsalgorithmus, die Schlüssellänge, oder ähnliche Parameter, die zur Verschlüsselung von Nutzdaten nötig sind, sein. Des weiteren wird durch die Anwendungshardware AHW über die Befehlsschnittstelle BS das Verfahren, also beispielsweise eine Verschlüsselung von Nutzdaten, gestartet.

Der Prozessor P steuert die administrativen Abläufe zur Verschlüsselung von Daten in dem Sicherheitschip SC und auch von im weiteren beschriebenen kryptographischen Protokollen.

Der Prozessor P transportiert jedoch nicht notwendigerweise die verschlüsselten, entschlüsselten bzw. mit kryptographischen Verfahren bearbeiteten Nutzdaten. Diese werden üblicherweise, falls nicht vom Prozessor P transportiert, über den chipinternen Datenbus DB transportiert und, was zu einem weiteren Vorteil des Sicherheitschips SC führt, daß die Verschlüsselungsleistung SC nicht abhängig ist von dem Prozessor P.

Außerdem wird durch die Abkopplung des chipinternen Datenbusses DS von dem chipinternen Bus IB gewährleistet, daß die internen Daten, die über den chipinternen Bus IB transportiert werden, an der Datenschnittstelle DS nicht abgehört oder manipuliert werden.

Dies führt zu einer wesentlichen Verbesserung der Sicherheitseigenschaften des Sicherheitschips SC gegenüber bekannten Sicherheitsmodulen, da sicherheitsrelevante Daten wie beispielsweise zur Verschlüsselung verwendete kryptographische Schlüssel nicht mehr von unbefugten abgehört werden können.

In dem Speicher SP werden sowohl nicht verschlüsselte als auch Daten, die zur Durchführung von Kryptoalgorithmen zwischengespeichert werden müssen, gespeichert, beispielsweise Zwischenschlüssel bei Verfahren, die nach dem Prinzip des exponentiellen Schlüsselaustausches arbeiten oder Zwischenschlüssel, die beim DES-Verfahren verwendet werden.

Weitere Algorithmenmodule AMi können vorgesehen sein zur Durchführung unterschiedlicher Sicherheitsdienste, beispielsweise von bekannten Authentifi-

kationsprotokollen oder auch zur Durchführung von Verfahren zum Schlüsselaustausch oder zur Schlüsselgenerierung kryptographischer Schlüssel.

Durch das Sensorikmodul SM werden physikalische Angriffe auf den Sicherheitschip SC detektiert, eventuell ausgewertet und über den chipinternen Bus IB an den Prozessor P gemeldet.

In dem Aktorikmodul AKM werden auf Anweisung des Prozessors P Schritte durchgeführt zur Abwehr von von dem Sensorikmodul SM detektierten Angriffen. Diese Sicherheitsmaßnahmen können zum Beispiel das Löschen aller zu dem Zeitpunkt in dem Speicher SP gespeicherten Daten sein.

Das Zeitgebermodul ZM weist mindestens folgende Komponenten auf:

- eine Zeitgeberschnittstelle SIO,
- einen Zeitgebercontroller ZC,
- eine Zählschaltung ZS, wobei die Zählschaltung ZS mindestens aufweist:
- einen Datenbuffer DB,
- einen Realzeitzähler RZ,
- eine Taktanpassung TA, und
- eine Zählerumschaltung ZU.

Das Zeitgebermodul ZM führt autonome Aufgaben beispielsweise zur Bereitstellung von Zeitstempeln aus. Die Zeitstempel werden über die Zeitgeberschnittstelle ZIO anderen Applikationen des Sicherheitschips SC zur Verfügung gestellt.

Der Zeitgebercontroller ZC übernimmt die Steuerung der Abläufe des Zeitgebermoduls ZM.

Die Zeitgeberschnittstelle ZIO stellt die Busschnittstelle des Zeitgebermoduls ZM zu dem chipinternen Bus IB dar. Die Zeitgeberschnittstelle ZIO wird in erster Linie benötigt, um die Kommunikation mit externen Controllern, im Falle des Sicherheitschips SC mit dem Prozessor P, abzuwickeln.

Vorgesehen sind also Anschlüsse zur Steuerung des Ablaufs des kryptographischen Kommunikationsprotokolls, also zur Steuerung der Kommunikation mit anderen Controllern, also mit dem Prozessor P. Weiterhin ist ein Anschluß vorgesehen, über den dem Zeitgebermodul ZM Manipulationsversuche, die durch das Sensorikmodul SM detektiert wurden, gemeldet werden, z. B. Manipulationen am Takt. Weitere Anschlüsse sind vorgesehen zum Austausch der Daten des Zeitgebermoduls ZM, also einer absoluten oder relativen Zeit, die durch das Zeitgebermodul ZM bestimmt wird.

In dem Zeitgebermodul ZM selbst werden keine Krypto-Algorithmen durchgeführt. Für die Abwicklung von Authentifikationsprotokollen und sonstigen Sicherheitsfunktionen sind die weiteren vorgesehenen Module des Sicherheitschip SC zuständig. Der Prozessor P muß entscheiden und überwachen, wer auf welche Weise über die Zeitgeberschnittstelle ZIO auf das Zeitgebermodul ZM zugreifen darf.

Der Zeitgebercontroller ZC übernimmt die Steuerung der Zeitgeberschnittstelle ZIO und der Zählschaltung ZS. Außerdem empfängt der Zeitgebercontroller ZC über die Zeitgeberschnittstelle ZIO logische Befehle von dem Prozessor P.

Die logischen Befehle des Prozessors P werden von dem Zeitgebercontroller ZC interpretiert und in die interne Steuerung des Zeitgebermoduls ZM umgesetzt. Somit überwacht der Zeitgebercontroller ZC den funktionalen Ablauf des gesamten Moduls. Er stellt somit das Steuerwerk des Zeitgebermoduls dar. Befehle, mit denen der Zeitgebercontroller ZC den Ablauf des Zeitgebermoduls ZM beeinflußt, können beispielsweise folgende Funktionen beinhalten:

- Stellen der Uhrzeit des Zeitgebermoduls ZM (Datum, Zeit, Synchronisationsmechanismus);
- Übernehmen von geladenen Uhrparametern in die aktuelle Uhrfunktion;
- Auslesen der Uhrzeit des Zeitgebermoduls ZM;
- Festlegen von Kalenderfunktionen (Monatsrhythmus, Berücksichtigen von Schaltjahren, Berücksichtigen der Sommerzeit, usw.);
- Festlegen von Uhr-Resetfunktionen, also Festlegen, ob ein Reset zu einer geordneten Zeit oder zu einer beliebigen Zeit stattfinden soll;
- Starten und Anhalten des Zeitgebermoduls ZM;
- Parametrieren der Taktanpassung TA, also Festlegen der Parameter, die zur Taktanpassung TA benötigt werden;
- Parametrieren der Auflösegenauigkeit des Zeitgebermoduls, das heißt die Einstellung, ob das Zeitgebermodul ZM die Zeit in Sekunden, in Millisekunden oder in Mikrosekunden messen soll;
- Parametrieren des Übertragungsformats der Uhrzeit des Zeitgebermoduls ZM;
- Auslesen von Statusinformation über das Zeitgebermodul ZM;
- Parametrieren des Zählmodus, also ob binär oder modulo gezählt werden soll;
- Ein- und Ausschalten eines Testmodus für das Zeitgebermodul ZM.

Außerdem wird durch den Zeitgebercontroller ZC eine Datenzugriffskontrolle und eine Funktionszugriffskontrolle durchgeführt. Darunter ist in diesem Zusammenhang beispielsweise zu verstehen:

- Zugriff auf das Zeitgebermodul ZM ist nur erlaubt nach einer erfolgreichen Prüfung einer Geheimnummer;
- Zugriff ist nur erlaubt nach erfolgreicher Authentifizierung;
- Zugriff ist nur lesend erlaubt;
- Zugriff ist nur schreibend erlaubt.

Die Zählschaltung ZS des Zeitgebermoduls ZM weist, wie im vorigen beschrieben, unter anderem den Realzeitzähler RZ auf.

Der Realzeitzähler RZ ist eine Zählschaltung, die aus kaskadierten Modulozählern aufgebaut ist. Die Kaskadierung und Synchronisation des Realzeitzählers RZ kann unter Berücksichtigung der Besonderheiten von Zeitsprüngen, zum Beispiel durch Sommerzeit oder durch Schaltjahre, usw. verursacht, geschehen. Für einige kryptographische Anwendungen ist eine Zählung der "relativen" Zeit, d. h. ein monoton zählender Binärzähler ausreichender Länge entsprechend der benötigten Zeit, weiterhin vorgesehen.

Die Taktanpassung TA dient der Erzeugung einer geeigneten Zeitbasis für die Zeitmessung bei dem Zeitgebermodul ZM bei externer Taktversorgung, wie dies beispielsweise bei heutzutage üblichen Chipkarten der Fall ist.

Der Datenbuffer DB dient zur Speicherung von Daten, die in dem Zeitgebermodul ZM benötigt werden.

Es ist weiterhin vorteilhaft, wenn die Algorithmenmodule AMi derart ausgelegt sind, daß die Schlüsselverwaltung direkt in Hardware unterstützt wird. Dies bie-

tet vor allem bei schnellen Schlüsselwechseln zwischen unterschiedlich verschlüsselten Datenströmen erhebliche Performancevorteile. Dies ist von besonderer Bedeutung im Bereich der paketorientierten Telekommunikation oder Datenverbindungen oder bei Applikations-Sharing-Systemen oder Multimedia-Anwendungen, beispielsweise in einem Local Area Network (LAN), bei dem viele Pakete zu unterschiedlichen Kommunikationspartnern übertragen und unterschiedlich kryptographisch bearbeitet werden müssen.

Patentansprüche

1. Sicherheitschip (SC),
   - bei dem der Sicherheitschip (SC) nur über eine Datenschnittstelle (DS) und über eine Befehlsschnittstelle (BS) mit einer Anwendungshardware (AHW) gekoppelt ist,
   - bei dem ein Prozessor (P) vorgesehen ist,
   - bei dem eine Vielzahl (VZ) von unabhängigen Algorithmenmodulen (AMi, i = 1 .. n) zur Durchführung von Verschlüsselungsalgorithmen vorgesehen ist, wobei die unabhängigen Algorithmenmodulen (AMi) über einen chipinternen Bus (IB) mit dem Prozessor (P) gekoppelt sind und über einen chipinternen Datenbus (DB) mit der Datenschnittstelle (DS) gekoppelt sind, und
   - bei dem ein Speicher (SP) vorgesehen ist, der mit dem chipinternen Bus (IB) gekoppelt ist.

2. Sicherheitschip (SC) nach Anspruch 1, bei dem mindestens ein Algorithmenmodul (AMi) der Vielzahl (VZ) der Algorithmenmodule (AMi) vorgesehen ist zur Durchführung symmetrischer Verschlüsselungsalgorithmen (SV).

3. Sicherheitschip (SC) nach Anspruch 1 oder 2, bei dem mindestens ein Algorithmenmodul (AMi) der Vielzahl (VZ) der Algorithmenmodule (AMi) vorgesehen ist zur Durchführung asymmetrischer Verschlüsselungsalgorithmen (AV).

4. Sicherheitschip (SC) nach einem der Ansprüche 1 bis 3, bei dem ein Zeitgebermodul (ZM) vorgesehen ist, das eine verläßliche absolute Zeit und/oder eine verläßliche relative Zeit ermittelt und zur Verfügung stellt.

5. Sicherheitschip (SC) nach einem der Ansprüche 1 bis 4, bei dem ein Sensorikmodul (SM) und/oder ein Aktorikmodul (AKM) vorgesehen ist zur Detektion und von Angriffen auf den Sicherheitschip (SC) und/oder zur Durchführung von Sicherheitsmaßnahmen bei erkannten Angriffen auf den Sicherheitschip (SC).

6. Sicherheitschip (SC) nach einem der Ansprüche 1 bis 5, bei dem weitere Module vorgesehen sind zur Durchführung weiterer Sicherheitsdienste.

7. Sicherheitschip (SC) nach einem der Ansprüche 1 bis 6, bei dem die Algorithmenmodule (AMi) derart ausgelegt sind, daß eine Schlüsselverwaltung direkt in Hardware unterstützt wird.

Hierzu 3 Seite(n) Zeichnungen

Nummer: DE 195 39 700 C1
Int. Cl.[6]: G 06 F 19/00
Veröffentlichungstag: 28. November 1996

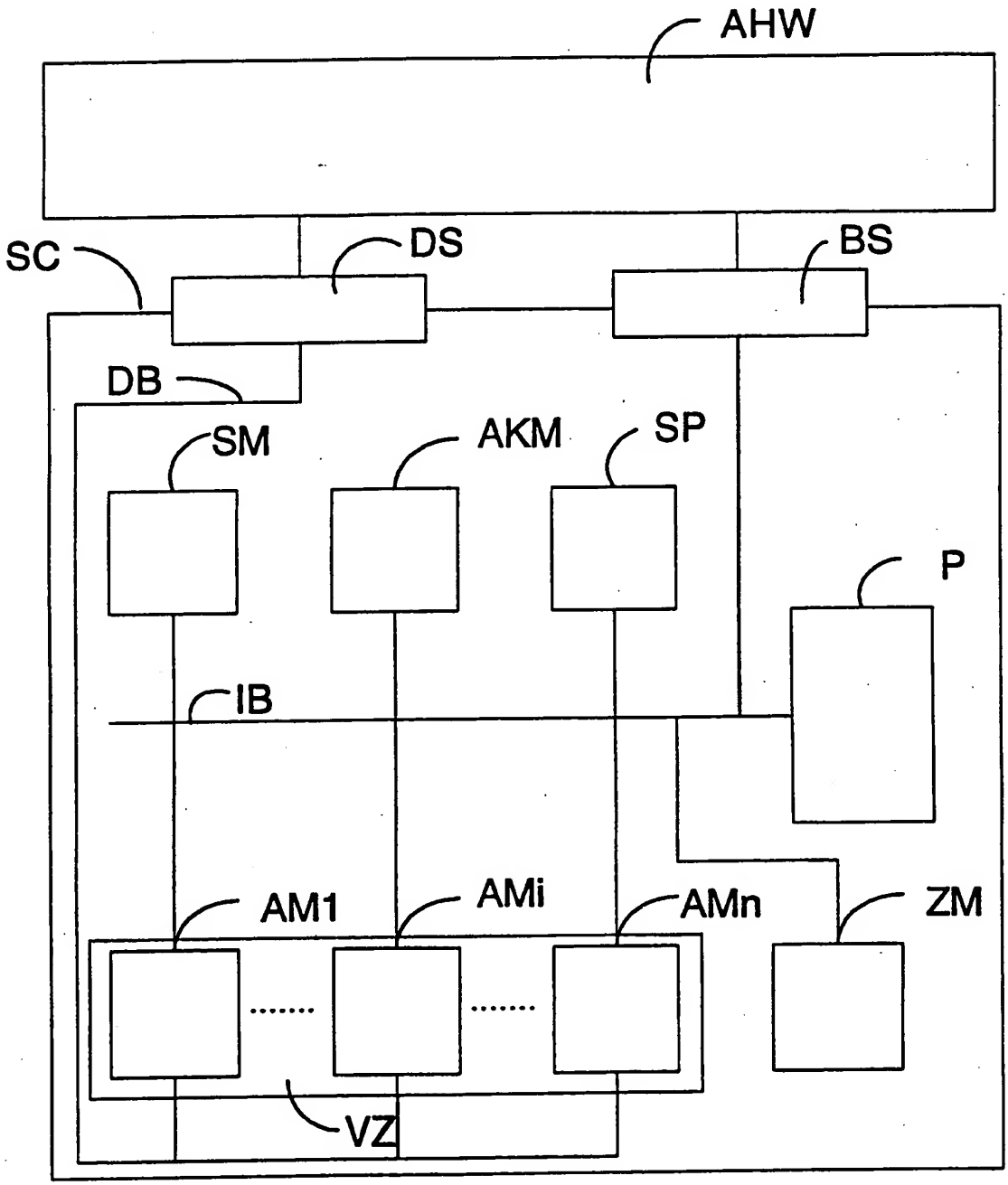


Fig. 1

Nummer: DE 195 39 700 C1
Int. Cl.[6]: G 06 F 19/00
Veröffentlichungstag: 28. November 1996

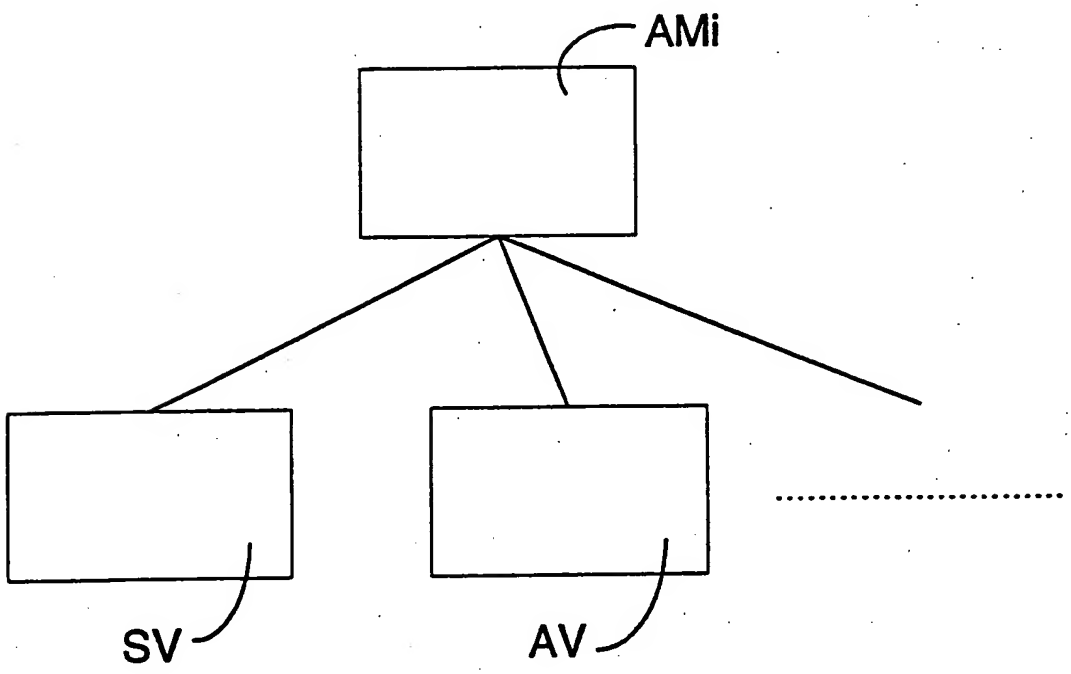


Fig. 2

Nummer: DE 195 39 700 C1
Int. Cl.[6]: G 06 F 19/00
Veröffentlichungstag: 28. November 1996

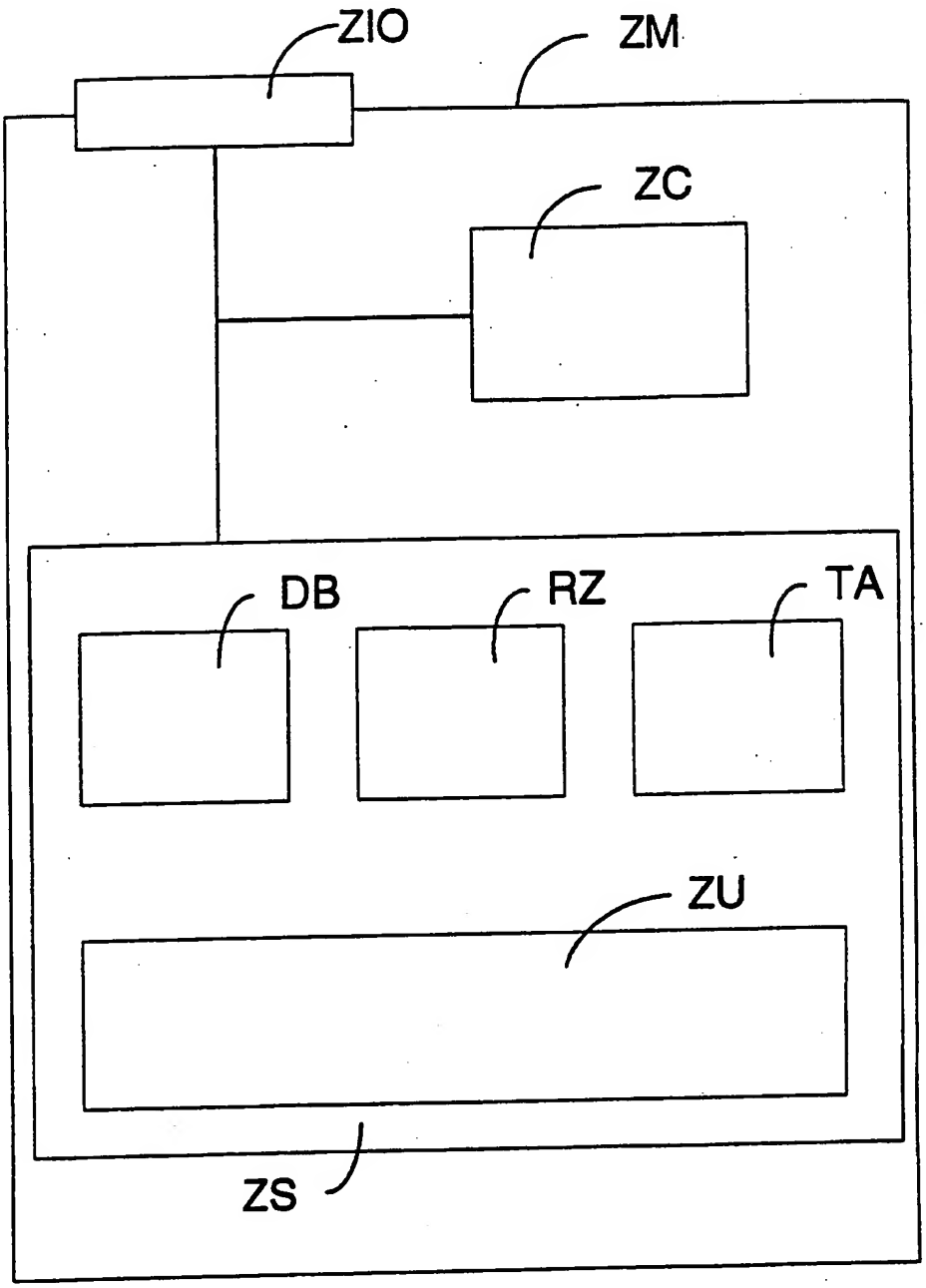


Fig. 3